Frequently Asked Questions:
Identity Theft Red Flags and Address Discrepancies

The staff of the Board of Governors of the Federal Reserve System ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), National Credit Union Administration ("NCUA"), Office of the Comptroller of the Currency ("OCC"), Office of Thrift Supervision ("OTS") (collectively the "Federal Financial Institution Regulatory Agencies") and the Federal Trade Commission ("FTC") (collectively "Agencies") have developed these frequently asked questions ("FAQs") to assist financial institutions, creditors, users of consumer reports, and card issuers in complying with the final rulemaking on Identity Theft Red Flags and Address Discrepancies implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), 15 U.S.C. § 1681m, and section 315 of the FACT Act, 15 U.S.C. § 1681c, that amended the Fair Credit Reporting Act (FCRA).[1]

Many of the questions the Agencies have received are answered in the supplemental information to the final rules.[2] These FAQs elaborate on the supplemental information where additional clarification is necessary and also explain the staff's view of how select provisions of the rulemaking apply to situations that were not specifically addressed in the final rules or supplemental information. Staff may supplement or revise these FAQs as necessary or appropriate in light of further questions and experience. The FTC will be issuing additional FAQs to answer questions specific to entities under FTC jurisdiction.

These FAQs do not address the applicability of any other Federal or state laws.

I. General FAQs

1. Do the Red Flags Rules, Card Issuers' Rules, or Address Discrepancy Rules contain record retention requirements?

These three Rules do not contain specific record retention requirements. However, financial institutions and creditors must be able to demonstrate that they have complied with the requirements of the Red Flags and Card Issuers' Rules, and users of consumer reports must be able to demonstrate that they have complied with the requirements of the Address Discrepancy Rules, in addition to any other applicable record retention requirements.

II. Identity Theft Red Flags (Red Flags Rules and Guidelines)[3]

A. Scope

[1] 12 C.F.R. part 41 (OCC); 12 C.F.R. part 222 (FRB); 12 C.F.R. parts 334 and 364 (FDIC); 12 C.F.R. part 571 (OTS); 12 C.F.R. part 717 (NCUA); and 16 C.F.R. part 681 (FTC). The FTC recently renumbered the sections in 16 C.F.R. part 681 as follows: the Address Discrepancy rule (originally § 681.1) was renumbered as § 641.1; the Red Flags rule (originally § 681.2) was renumbered as § 681.1; and the Card Issuers' rule (originally § 681.3) was renumbered as § 681.2. For ease of reference, these FAQs refer to the original numbering scheme.
[2] See 72 Fed. Reg. 63718 (Nov. 9, 2007).
[3] 12 C.F.R. § __.90 and 16 C.F.R. § 681.2. (Section citations reference the uniformly numbered rules issued by the Federal Financial Institution Regulatory Agencies and the rules issued by the FTC.)

1. What is the relationship between the information security standards[4] issued by the Agencies and the Red Flags Rules and Guidelines?

The information security standards help to reduce identity theft ("a fraud committed or attempted using the identifying information of another person without authority") by keeping individuals' sensitive data from falling into the hands of an identity thief. The information security standards require financial institutions to have reasonable policies and procedures that are designed to safeguard customer information and protect it from unauthorized access or misuse and to ensure the proper disposal of customer and consumer information.

By contrast, the Red Flags Rules and Guidelines seek to ensure that financial institutions and creditors are alert for signs or indicators that an identity thief is actively misusing another individual's sensitive data, typically to obtain products or services from the institution or creditor. The Red Flags Rules require financial institutions and creditors that offer or maintain "covered accounts" to have policies and procedures to identify patterns, practices, or activities that indicate the possible existence of identity theft, to detect whether identity theft may be occurring in connection with the opening of a covered account or an existing covered account, and to respond appropriately.

2. Do the Red Flags Rules and Guidelines apply to all banks, savings associations, and credit unions, or only those that directly or indirectly hold transaction accounts belonging to consumers?

The Red Flags Rules and Guidelines implement section 114 of the FACT Act, 15 U.S.C. § 1681m, which applies to "financial institutions" and "creditors."[5] The FCRA definition of "financial institution" applies to: (1) all banks, savings associations, and credit unions, regardless of whether they hold a transaction account belonging to a consumer; and (2) any other person that directly or indirectly holds a transaction account belonging to a consumer. Accordingly, all banks, savings associations, and credit unions are covered by the Red Flags Rules and Guidelines as "financial institutions," whether or not they hold a transaction account belonging to a consumer.

3. Do the Red Flags Rules and Guidelines apply to banks and savings associations whose powers are limited to trust activities?

Yes. As described above, the Red Flags Rules and Guidelines apply to "financial institutions" as defined in the FCRA. Therefore, all banks and savings associations, including those whose powers are limited to trust activities, are covered by the Red Flags Rules and Guidelines.

---

[4] 12 C.F.R. part 30, app. B (OCC); 12 C.F.R. part 208, app. D-2 and Part 225, app. F (FRB); 12 C.F.R. part 364, app. B (FDIC); 12 C.F.R. part 570, app. B (OTS); 12 C.F.R. part 748, appendix A (NCUA); and 16 C.F.R. 314 (FTC).

[5] Section 114 of the FACT Act amended section 615 of the FCRA.

4. Do the Red Flags Rules and Guidelines apply to the foreign branches of U.S. banks?[6]

No. The FCRA, like many federal consumer protection laws, does not expressly address extraterritorial applicability. Because a foreign branch of a U.S. bank is not an entity located in the United States, the Red Flags Rules and Guidelines do not apply. This conclusion is consistent with a number of consumer protection regulations that exclude foreign branches of U.S. banks from coverage. See Regulation Z, Official Staff Commentary, 12 C.F.R. part 226, supplement I, § 226.1(c)-1; Regulation E, Official Staff Commentary, 12 C.F.R. part 205, supplement I, § 205.3(a)-2; Regulation M, Official Staff Commentary, 12 C.F.R. part 213, supplement I, § 213.1-1. Other regulations that impose customer information collection and verification requirements, such as the Customer Identification Program regulations implementing the USA PATRIOT Act, do not apply extraterritorially. See 31 C.F.R. § 103.121.

Nevertheless, as a matter of safety and soundness, financial institutions are strongly encouraged to implement an effective identity theft prevention program throughout their operations, including in their foreign offices, consistent with local laws.

5. What are "functionally regulated" subsidiaries of banks and savings associations that are referenced in the scope sections of the Identity Theft Red Flags regulations issued by several of the Agencies?

The term "functionally regulated subsidiary" is defined in section 5(c)(5) of the Bank Holding Company Act of 1956, as amended by the Gramm-Leach-Bliley Act (12 U.S.C. § 1844(c)). The term means any company that is not a bank holding company or depository institution and that is:

- a broker or dealer that is registered under the Securities Exchange Act of 1934;
- a registered investment adviser, properly registered by or on behalf of either the Securities and Exchange Commission or any state, with respect to the investment advisory activities of such investment adviser and activities incidental to such investment advisory activities;
- an investment company that is registered under the Investment Company Act of 1940;
- an insurance company, with respect to insurance activities of the insurance company and activities incidental to such insurance activities, that is subject to supervision by a state insurance regulator; or
- an entity that is subject to regulation by the Commodity Futures Trading Commission, with respect to the commodities activities of such entity and activities incidental to such commodities activities.

6. Are brokers, dealers, investment advisors, or investment or insurance companies, including those that are subsidiaries of a bank or savings association, covered by the Red Flags Rules and Guidelines?

[6] The FTC will address this issue similarly for the foreign subsidiaries of entities under FTC jurisdiction in the separate FAQs it will be issuing as referenced above.

A broker, dealer, investment advisor, or investment or insurance company that is a "financial institution" or "creditor" under the FCRA is covered by the Red Flags Rules and Guidelines issued by the FTC, including any such entity that is a subsidiary of a bank or savings association.

7. Are corporate credit unions covered by the Red Flags Rules and Guidelines?

Yes. The term "corporate credit union" is defined in 12 C.F.R. § 704.2 and means a credit union chartered under Federal or state law that:

- receives shares from and provides loan services to credit unions;
- is operated primarily for the purpose of serving other credit unions;
- is designated by the NCUA as a corporate credit union;
- limits natural person members to the minimum required by state or federal law to charter and operate the credit union; and
- does not condition the eligibility of any credit union to become a member on that credit union's membership in any other organization.

As described above in II.A.2, the Red Flags Rules and Guidelines apply to "financial institutions" as defined in the FCRA, regardless of whether they hold consumer transaction accounts. Therefore, all credit unions, including corporate credit unions, are covered by the Red Flags Rules and Guidelines.

8. Are credit union service organizations (CUSOs) covered by the Red Flags Rules and Guidelines?

CUSOs, according to the Federal Credit Union Act, provide "services which are associated with the routine operations of credit unions" and are "established primarily to serve the needs of its member credit unions, and whose business relates to the daily operations of the credit unions they serve." 12 U.S.C. §§ 1757(5)(D), (7)(I). A CUSO that is a "creditor" under the FCRA is covered by the Red Flags Rules and Guidelines issued by the FTC.

B. <u>Definitions</u>

<u>Covered Account</u>

1. What is a "covered account?"

The term "account" is defined in the Red Flags Rules as "a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes." The definition of "covered account" is divided into two parts. The first part refers to "an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions." An account that meets this part of the definition is always a covered account.

The second part of the definition refers to "any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the

safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." Therefore, an account that does not meet the first part of the definition may still be a "covered account" if it poses a reasonably foreseeable risk to consumers or to the financial institution or creditor from identity theft. Due to the risk-based nature of this part of the definition, each financial institution or creditor must determine which of its accounts, if any, meet this definition and, therefore, must be covered by its Identity Theft Prevention Program. This determination should be based upon a risk evaluation that includes consideration of the methods the institution or creditor provides to open its accounts, the methods it provides to access such accounts, and its previous experience with identity theft.

2. Under what circumstances are business accounts "covered accounts?"

Business accounts are "accounts" if they establish a continuing relationship between a person and a financial institution or creditor to obtain a product or service for business purposes. The FCRA definition of person, 15 U.S.C. § 1681a(b), is not limited to individuals. However, business accounts are not covered by the first part of the definition of "covered account" (set out above under II.B.1) because they are not primarily for personal, family, or household purposes.

Instead, each financial institution or creditor must determine which of its business accounts, if any, present a reasonably foreseeable risk of identity theft under the second part of the definition of a "covered account." For example, the accounts of small businesses or sole proprietorships may be particularly vulnerable to identity theft.

3. Does a financial institution or creditor that makes a small business loan that is guaranteed by a consumer have a "covered account" with that consumer?

A guarantor of a small business loan establishes a continuing relationship with a financial institution or creditor because the individual assumes secondary liability on the loan he or she guarantees and thereby receives an extension of credit. However, a business loan guaranteed by a consumer is not covered by the first part of the definition of "covered account" (set out above under II.B.1) because it is not primarily for personal, family, or household purposes. Instead, each financial institution or creditor must determine whether a business loan guaranteed by a consumer presents a reasonably foreseeable risk of identity theft under the second part of the definition of a "covered account."

4. To what extent do pre-paid card products fall within the definition of "covered account?"

There are various types of pre-paid cards. Whether a certain type of pre-paid card is an "account" and a "covered account" will depend on the specific features of the card and the risks associated with the card.

Some pre-paid cards do not provide for a continuing relationship between a consumer who obtains the card from the issuer and the financial institution that issues the card, or between the person who receives and uses the card and the financial institution. For example, many gift cards

are issued without the creation of any record of the person who obtains the card or the recipient of the card. Such gift cards would not establish a continuing relationship with the issuing financial institution, and therefore are generally not "accounts" or "covered accounts."

By contrast, other pre-paid cards are offered primarily for personal, family, or household purposes, permit multiple transactions, and create a continuing relationship between the person who obtains and/or uses the pre-paid card and the financial institution that issues the card. For example, payroll cards generally meet these criteria and therefore qualify as "covered accounts" under the first part of the definition (set out above under II.B.1).

5. Is a certificate of deposit a "covered account?"

A certificate of deposit is an "account" because it involves a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Whether a certificate of deposit is a "covered account" will depend on its features and risks. For example, a certificate of deposit purchased by a consumer that does not involve, and is not designed to permit, multiple payments or transactions, is not covered under the first part of the definition of a "covered account" (set out above under II.B.1). Therefore, the financial institution must determine for itself whether the certificate of deposit presents a reasonably foreseeable risk of identity theft under the second part of the definition of a "covered account."

6. To what extent does an individual retirement account (IRA) fall within the definition of "covered account?"

An IRA is an "account" because it involves a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Generally, IRAs will qualify as a "covered account" under the first part of the definition of a "covered account" (set out above under II.B.1) if offered by a financial institution or creditor. First, an IRA is offered primarily for personal, family, or household purposes. In addition, IRA accounts involve, and are designed to permit, multiple payments or transactions both during the accumulation phase when periodic contributions are made, and during the withdrawal phase when periodic withdrawals are made, as well as transactions (such as mutual fund investments) within the account itself.

7. To what extent does a trust account fall within the definition of "covered account?"

There are many types of trust accounts, which may be established for business or consumer purposes. The features and risks of a trust account will determine whether it is a "covered account."

For instance, a trust account may constitute an "account" because it involves a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Such a trust account will qualify as a "covered account" under the first part of the definition of a "covered account" (set out above under II.B.1) if it is offered primarily for personal, family, or household purposes and it involves

or is designed to permit multiple payments or transactions, such as deposits by the grantor, stock trades, and payments to beneficiaries. For other types of trust accounts, such as business trust accounts, each financial institution or creditor must determine whether the account presents a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, as required under the second part of the definition of "covered account."

8. Does the term "covered account" include accounts established in the U.S. by non-U.S. residents?

Yes. The term "covered account" includes all accounts located in the U.S., including those established by non-U.S. residents. While section 615(e) of the FCRA does not expressly address this question, it directs the Agencies to prescribe regulations and guidelines that relate to "risks to account holders or customers or to the safety and soundness of the institution or [creditor]." Thus, section 615(e) of the FCRA serves both a consumer protection purpose and a safety and soundness purpose.

Federal consumer protection regulations take different approaches with regard to accounts established by non-U.S. residents. However, regulations and examinations related to safety and soundness and other matters generally consider the risks posed by all activities undertaken and accounts held by an institution, including activities undertaken with and accounts opened by non-U.S. residents. For example, the Customer Identification Program regulations implementing the USA PATRIOT Act encompass customer information collection and identity verification procedures for both U.S. persons and non-U.S. persons opening an account with a financial institution. See 31 C.F.R. § 103.121.

Therefore, in light of the fact that section 615(e) of the FCRA includes a safety and soundness component that requires financial institutions and creditors to protect themselves from identity theft perpetrated in connection with all accounts located in the U.S., the term "covered account" applies to accounts opened and maintained in the U.S. by non-U.S. residents, as well as by U.S. residents.

9. How do the Red Flags Rules apply to indirect lending? Is a consumer loan that is purchased by the financial institution or creditor (e.g., a mortgage loan or car loan) a "covered account?"

A consumer loan, such as a mortgage or auto loan, is covered under the first part of the "covered account" definition (set out above under II.B.1) to the extent that it is "an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions."

In the case of such loans, the financial institution or creditor that initially extends credit to the consumer is responsible for applying its Identity Theft Prevention Program to the opening of that covered account. If that loan is purchased by another financial institution or creditor, then that entity becomes responsible for applying its Identity Theft Prevention Program to the loan as an existing covered account.

10. Is a lease offered by a financial institution or creditor a "covered account?"

A lease offered by a financial institution or creditor is an "account" because it involves a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Whether a lease is a "covered account" will depend on its features and risks. For instance, a lease offered to a consumer by a financial institution or creditor will qualify as a "covered account" under the first part of the definition of "covered account" (set out above under II.B.1). In contrast, a business-purpose lease is not covered by the first part of the definition because it is not primarily for personal, family, or household purposes. Instead, each financial institution or creditor must determine which of its business leases, if any, present a reasonably foreseeable risk of identity theft under the second part of the definition of "covered account."

Identity Theft

11. Is check forgery or use of a stolen credit card "identity theft?"

Yes. The final rules define identity theft with reference to the FTC's regulation, 16 C.F.R. § 603.2(a), which provides that the term "identity theft" means "a fraud committed or attempted using the identifying information of another person without authority." The FTC defines the term "identifying information" to mean:

> any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any-
>
> 1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
> 2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
> 3) Unique electronic identification number, address, or routing code; or
> 4) Telecommunication identifying information or access device (as defined in 18 U.S.C. § 1029(e)).

Thus, under the FTC's regulation, the creation of a fictitious identity using any single piece of information belonging to a real person, such as check forgery or the use of a stolen credit card, falls within the definition of "identity theft" because such a fraud involves "using the identifying information of another person without authority."

C. Establishment of an Identity Theft Prevention Program ("Program")

1. Is a financial institution or creditor required to educate consumers regarding the prevention of identity theft as a part of its Program?

The Red Flags Rules do not require a financial institution or creditor to educate consumers regarding the prevention of identity theft. However, consumer education programs may be helpful as part of an overall effort to address the problem of identity theft.

D. Elements of the Program

Detect Red Flags

1. To what extent can a financial institution or creditor use an automated solution to satisfy the requirement to detect red flags?

The final Red Flags Rules do not require the use of any specific technology, systems, processes, or methodology. Financial institutions and creditors may use automated solutions if they effectively detect red flags in connection with account openings and existing covered accounts, but are not required to do so.

An automated system, however, may have to be supplemented by other policies and procedures that do not rely upon automation. For example, in some instances, the detection of fraudulent or altered identifying documentation may require the manual review of those documents by employees of a financial institution or creditor.

Respond appropriately to Red Flags detected

2. If a financial institution or creditor detects Red Flags and, as a result, suspects that an applicant is an identity thief, what response do the Red Flags Rules require?

The Red Flags Rules state that the Program of a financial institution or creditor must include policies and procedures for appropriately responding to identity theft that are commensurate with the degree of risk posed. The Rules do not require a specific response to any particular situation but provide an illustrative list of appropriate responses. Appropriate responses to the situation described above could include not opening the account, filing a suspicious activity report ("SAR") (for those financial institutions and creditors that are subject to SAR rules), notifying law enforcement, and/or contacting the customer whose identity has been stolen. See 12 C.F.R. § __.90(d)(2)(iii) and 16 C.F.R. § 681.2(d)(2)(iii).

E. Administration of the Program

1. Do the Red Flags Rules require financial institutions or creditors to oversee all service provider arrangements or only those service providers that offer fraud detection services?

The obligation to oversee service provider arrangements is not limited to service providers that offer fraud detection services. The oversight requirement applies when the financial institution or creditor engages a service provider to perform an activity in connection with opening or accessing one or more covered accounts. The oversight obligation is intended to ensure that the financial institution or creditor is responsible for complying with the Red Flags Rules, even if it

outsources one or more of its account opening or access activities to a third-party service provider.

For example, a service provider that provides an online banking platform permitting account opening or access, performs call center services that permit account access, or collects debts on delinquent accounts, would be providing services related to covered accounts to the financial institution or creditor. In such cases, the financial institution or creditor should take steps to ensure that the activities of such service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft in accordance with the Red Flags Rules. The oversight requirement does not require a service provider to have the same Program as the financial institution or creditor. The Red Flags Guidelines enable flexible business arrangements so that financial institutions and creditors may use service providers that have developed their own Programs, as long as the service provider's Program is sufficient to meet the financial institution's or creditor's obligations under the Red Flags Rules. However, a financial institution or creditor must still maintain its own Program that meets the requirements of the Red Flags Rules, including the oversight requirement.

2. Do the Red Flags Rules require oversight of service provider arrangements through written contracts?

The Red Flags Rules do not specifically require the financial institution's or creditor's oversight of the service provider to be maintained through a written contract. However, the Red Flags Guidelines state that a financial institution or creditor is responsible for ensuring the service provider's compliance with the Red Flags Rules. Financial institutions or creditors may find it helpful to require a service provider, by contract, to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities and either report the red flags to the financial institution or creditor or take its own appropriate steps to prevent or mitigate identity theft. See Section VI(c) of the Guidelines.

F. Examples of Red Flags[7]

1. The Red Flags Rules require a financial institution or creditor to consider the Guidelines and adopt those that are appropriate. Does this requirement also apply to the list of red flags in the supplement to the Guidelines?

The preamble language in Supplement A provides only that a financial institution or creditor "may" consider incorporating into its Program the examples of red flags. There is no requirement that they do so. A financial institution or creditor may find that none or only some of these examples are relevant to its business. These examples also may only be relevant when combined or with other indicators of identity theft. The preamble language notes that a financial institution's or creditor's compliance with the rules will be determined based on the overall effectiveness of its Program, which must be appropriate to its size and complexity and the nature and scope of its activities, and not on whether the institution or creditor did or did not include specific red flags from the list of examples. Furthermore, these examples are not intended to be a comprehensive list of red flags.

[7] Supplement A to Appendix J and Supplement A to Appendix A.

III. Duties of Card Issuers Regarding Changes of Address (Card Issuers' Rules)[8]

A. Address validation requirements

1. Can a card issuer rely upon the US Postal Service's change of address procedures to validate a change of address for purposes of the Card Issuers' Rules?

The fact that a card issuer received a change of address notice from the US Postal Service is not sufficient to satisfy the validation requirements of the Card Issuers' Rules. A card issuer that receives a notice of a change of address from the postal system regarding a cardholder's address, and, within at least 30 days, a request for an additional or replacement card, may not issue the card unless it has validated the cardholder's address using one of the procedures set forth in the Card Issuers' Rules.

2. Do the address validation requirements of the Card Issuers' Rules apply to corporate credit or debit cards?

There are many types of corporate credit and debit cards with many possible combinations of features. For example, a card may be in the name of a corporation or an individual employee, and the corporation or individual employee may be responsible for payment.

The address validation requirements in the Card Issuers' Rules apply when a card issuer receives a "notification of a change of address for a *consumer's* debit or credit card account" followed by a request for an additional or replacement card." (Emphasis added). Identity theft in connection with a card that a consumer uses for a business purpose may affect the consumer's personal credit standing. Therefore, the address validation requirements of the Card Issuers' Rules extend to debit and credit cards that are in an individual employee's name and for which the employee is responsible for payment.

IV. Duties of Users Regarding Address Discrepancies (Address Discrepancy Rules)[9]

A. Scope

1. What is a "notice of address discrepancy?"

A "notice of address discrepancy" is a notice sent to a user of a consumer report by a nationwide consumer reporting agency ("NCRA") notifying the user that the address provided by the user to obtain the report "substantially differs" from the address the NCRA has in the consumer's file. The FCRA does not define the phrase "substantially differs" nor does it direct the Agencies to define this phrase as a part of the rulemaking on address discrepancies.

2. Do the requirements of the Address Discrepancy Rules apply to all notices of discrepancy received from *any* consumer reporting agency?

---

[8] 12 C.F.R. § __.91 and 16 C.F.R. § 681.3.
[9] 12 C.F.R. § __.82 and 16 C.F.R. § 681.1.

No. The Address Discrepancy Rules only apply to notices of address discrepancy received from an NCRA, which is defined in Section 603(p) of the FCRA, 15 U.S.C. § 1681a(p), as a consumer reporting agency that regularly engages in assembling or evaluating, and maintaining, public record and credit account information for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, regarding consumers residing nationwide. There are only three NCRAs – Experian, Equifax, and TransUnion. Consequently, the Address Discrepancy Rules currently apply only to notices of address discrepancy received from these three NCRAs, either directly or from a third party reseller or procurer acting on behalf of an NCRA (see IV.A.3 below).

A notification of address discrepancy received from an entity that is not an NCRA, however, may be a red flag for purposes of the Red Flags Rules.

3. How do the Address Discrepancy Rules apply to a reseller or other person that obtains consumer reports from one or more of the three NCRAs for purposes of resale?

A user of consumer reports that receives a notice of address discrepancy from a reseller or other person that procures consumer reports for resale ("procurer") from one or more of the three NCRAs must comply with applicable portions of the Address Discrepancy Rules. In these circumstances, the reseller or procurer is acting on behalf of the NCRA.

For all notices of address discrepancy received from such resellers or procurers, the user would be obligated to develop and implement reasonable policies and procedures to enable it to form a reasonable belief that the consumer report relates to the consumer about whom it has requested the report. However, the user must have reasonable policies and procedures to furnish the consumer's confirmed address to an NCRA only if the three-prong test set out in 12 C.F.R. § __.82(d) and 16 C.F.R. § 681.1(d) of the Address Discrepancy Rules (discussed below in IV.C.1) applies: in other words, only if (1) the user regularly and in the ordinary course of business furnishes information to the NCRA from which the notice of address discrepancy was obtained by the reseller or procurer, (2) the user can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report, and (3) the user establishes a continuing relationship with the consumer. If the consumer report does not indicate from which NCRA the notice of address discrepancy was obtained (for example, in the case of a merged report), the user's reasonable policies and procedures would not need to provide for the furnishing of confirmed addresses.

4. What is the relationship between the Address Discrepancy Rules and the Red Flags Rules?

There is very little relationship between the substantive provisions of the Address Discrepancy Rules and the Red Flags Rules. The primary purpose of the Address Discrepancy Rules is to enhance the accuracy of consumer reports, while the objective of the Red Flags Rules is to detect and prevent identity theft. Also, the two rules cover different categories of entities. The Address Discrepancy Rules apply to <u>users of consumer reports</u>, while the Red Flags Rules apply to <u>financial institutions and creditors</u>.

The Address Discrepancy Rules focus on whether a notice of address discrepancy may be an indication that a user of a consumer report does not have the correct consumer report for the consumer about whom it requested the report and require the user to provide a confirmed address to the NCRA that supplied the report. However, in some instances, for users of consumer reports that are financial institutions or creditors covered by the Red Flags Rules, that notice of address discrepancy also may be an indication of identity theft and is therefore listed as an example of an identity theft red flag in the supplement to the Red Flags Guidelines.

B. <u>Requirement to establish a reasonable belief</u>

1. If the consumer withdraws his or her application to open a new account, must a user that receives a notice of address discrepancy take steps to establish a reasonable belief that the consumer report relates to the consumer?

No. The user is not required to take any additional steps in these circumstances.

2. If the user plans to deny the consumer's application to open a new account on the basis of information in a consumer report, must a user that receives a notice of address discrepancy take steps to establish a reasonable belief that the consumer report it has obtained relates to the consumer?

Yes. If a user plans to deny the consumer's application based on a consumer report, the user must take steps to ensure that the consumer report on which it is relying pertains to the consumer.

C. <u>Requirement to furnish consumer's address to a consumer reporting agency</u>

1. A user "regularly and in the ordinary course of business" furnishes information to an NCRA regarding all of its consumer loans. Is the user required to furnish a confirmed address to the NCRA if the user receives a notice of address discrepancy in connection with an application for a car loan submitted by a consumer who already has a mortgage loan with the user?

According to 12 C.F.R.§ __.82(d) and 16 C.F.R. § 681.1(d) of the Address Discrepancy Rules, a user must have reasonable policies and procedures to furnish a consumer's confirmed address to a consumer reporting agency if the user: (1) can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report; (2) establishes a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained. If the three prongs of this test are met, the user must have reasonable policies and procedures to furnish a confirmed address to the NCRA that provided the consumer report. The user must comply with this requirement each time that it enters into a continuing relationship with a consumer, regardless of whether the consumer is an existing customer.

Accordingly, the fact that a consumer may have an existing mortgage loan with the user has no bearing on whether the user must furnish a confirmed address to the NCRA when the consumer obtains the car loan. Instead, if the consumer receives the car loan, thereby establishing a relationship between the user and the consumer, and the user can form a reasonable belief that the consumer report relates to the consumer, then the user would be expected to furnish the confirmed address. However, if the consumer does not receive the car loan, a new relationship is not established with the consumer and the user is not required to furnish a confirmed address in connection with the car loan according to 12 C.F.R. § __.82 and 16 C.F.R. § 681.1.

2. The NCRAs have provided a specific code in their reporting formats that permits a user to indicate that it is furnishing a confirmed address for a consumer. Do the Address Discrepancy Rules require a user to use this field and "flag" that it is furnishing a confirmed address?

The Address Discrepancy Rules only require users to develop and implement reasonable policies and procedures for furnishing confirmed addresses. The Rules do not require users to specially indicate that they are furnishing a confirmed address for the consumer or otherwise specify what mechanism must be used to furnish those confirmed addresses. However, users may use this code when furnishing a confirmed address to an NCRA.

3. Is a user furnishing information "regularly and in the ordinary course of business" if the user only furnishes information to an NCRA regarding delinquent accounts?

Whether a user regularly and in the ordinary course of business furnishes information to an NCRA does not depend upon the type or comprehensiveness of the information that the user regularly reports. If the user regularly and in the ordinary course of business furnishes information to the NCRA from which it received the notice of address discrepancy and the other two prongs of 12 C.F.R. § __.82(d) and 16 C.F.R. § 681.1(d) (set out above under IV.C.1) are met, then the user must have reasonable policies and procedures to furnish a confirmed address to the NCRA from which it received the notice of address discrepancy.

A user that only infrequently reports delinquent information (e.g., a small landlord that reports on delinquent tenants on an ad hoc basis) generally would not be considered to be reporting regularly and in the ordinary course of business.